# 在FireSIGHT系统上配置LDAP身份验证对象

## 目录

<u>简介</u> <u>LDAP身份验证对象的配置</u> <u>相关文档</u>

## 简介

身份验证对象是外部身份验证服务器的服务器配置文件,包含这些服务器的连接设置和身份验证过 滤器设置。您可以在FireSIGHT管理中心上创建、管理和删除身份验证对象。本文档介绍如何在 FireSIGHT系统上配置LDAP身份验证对象。

## LDAP身份验证对象的配置

1.登录FireSIGHT管理中心的Web用户界面。

2.定位至**系统>本地>用户管理**。



**Login Authentication** 

单击Create Authentication Object。

Create Authentication Object	
<ul> <li>3.选择Authentication Method和Server Type。</li> <li>认证方法:LDAP</li> <li>名称: &lt;身份验证对象名称&gt;</li> <li>服务器类型:MS Active Directory</li> <li>注意:标有星号(*)的字段为必填字段。</li> </ul>	
Authentication Object Authentication Method Name * Description Server Type	LDAP 🗘

4.指定主服务器和备用服务器的主机名或IP地址。备份服务器是可选的。但是,同一域中的任何域 控制器都可以用作备份服务器。

注意:虽然LDAP端口默认为端口389,但您可以使用LDAP服务器侦听的非标准端口号。

5.指定LDAP特定参数,如下所示:

**提示:**应在配置LDAP特定参数之前识别用户、**组和OU属性**。请阅读<u>此文档</u>以识别用于身份 验证对象配置的Active Directory LDAP对象属性。

- •基础DN 域或特定OU DN
- Base Filter 用户所属的组DN。
- 用户名 DC的模拟帐户
- 密码: <password>
- •确认密码: <password>
- 高级选项:
  - •加密:SSL、TLS或无
  - SSL证书上传路径:上传CA认证(可选)
  - 用户名模板:%s
  - •超时(秒):30

LDAP-Specific Parameters			
Base DN *	DC=VirtualLab,DC=local	Fetch DNs	ex. dc=sourcefire,dc=com
Base Filter	(memberOf=CN=Secadmins,CN=Seci		ex. (cn=jsmith), (lcn=jsmith), (&(cn=jsmith)( (cn=bsmith) (cn=csmith*)))
User Name *	CN=sfdc1,CN=Service Accounts,DC		ex. cn=jsmith,dc=sourcefire,dc=com
Password *	•••••		
Confirm Password *	******		
Show Advanced Options	•		
Encryption	🗇 SSL 🗇 TLS 🖲 None		
SSL Certificate Upload Path	Browse.		ex. PEM Format (base64 encoded version of DER)
User Name Template	%s		ex. cn=%s,dc=sourcefire,dc=com
Timeout (Seconds)	30		

在AD的域安全策略设置中,如果LDAP服务器签名要求设置为需要签名,则必须使用SSL或TLS。

#### LDAP服务器签名要求

- •无:不需要数据签名即可与服务器绑定。如果客户端请求数据签名,则服务器支持它。
- •需要签名:除非使用TLS\SSL,否则必须协商LDAP数据签名选项。

**注意:**LDAPS不需要客户端或CA证书(CA证书)。但是,CA证书将上传到身份验证对象 ,这会增加安全级别。

#### 6.指定属性映射

#### • UI访问属性:sAMAccountName

• 外壳访问属性:sAMAccountName

#### Attribute Mapping

UI Access Attribute \*

Shell Access Attribute \*

**提示:**如果在测试输出中遇到不支持的用户消息,请将UI Access Attribute更改为 userPrincipalName,并确保User Name template设置为%s。

Unsupported Admin Users	The following administrator shell access users (3) were found with this filter but are invalid because their format is not supported for this appliance:		
	secadmin1 , secadmin3		
Unsupported Users	The following users (3) were found with this filter but are invalid because their format is not supported for this appliance:		
	secadmin1 , secadmin3		
	Save Test Cancel		

#### 7. 配置组控制的访问角色

在ldp.exe上,浏览到每个组,并将相应的组DN复制到身份验证对象,如下所示:

• <Group Name>组DN:<group dn>

•组成员属性:应始终为成员

示例:

•管理员组DN:CN=DC管理员,CN=安全组,DC=虚拟实验室,DC=本地

•组成员属性:成员

AD安全组的属性为**member**,后跟成员用户的DN。**member**属性前面的number表示成员用户的数量 。

3> member: CN=secadmin3, CN=Users, DC=VirtualLab, DC=local; CN=secadmin2, CN=Users, DC=VirtualLab, DC=local; CN=secadmin1, CN=Users, DC=VirtualLab, DC=local; CN=secadmin1, CN=Users, DC=VirtualLab, DC=local; CN=secadmin2, CN=se

8.选择**与外壳访问过滤器**的基本过滤器相同,或指定memberOf属性(如步骤5所示)。

**外壳访问过滤**器:(memberOf=<group DN>)

例如,

**外壳访问过滤**器:(memberOf=CN=Shell users,CN=安全组,DC=VirtualLab,DC=local)

9.保存身份验证对象并执行测试。成功的测试结果如下所示:

# Info

Administrator Shell Test:

3 administrator shell access users were found with this filter.

See Test Output for details.



User Test:

3 users were found with this filter. See Test Output for details.

## Success

Test Complete: You may enter a test user name to further verify your Base Filter parameter.

Admin Users	The following administrator shell access users (3) were found with this filter: 
Users	The following users (3) were found with this filter: secadmin1, secadmin2, secadmin3
*Required Field	
	Save Test Cancel

10.身份验证对象通过测试后,在系统策略中启用该对象,并将策略重新应用到设备。

## 相关文档

• <u>识别身份验证对象配置的Active Directory LDAP对象属性</u>

×

×

50